

-2-

IN THE CLAIMS

Amended claims follow. Insertions are underlined, while deletions are struck out. The status of each claim is included prior to each heading.

1. (Currently Amended) A method for managing security policies in a distributed computing system, wherein security policies determine access rights to a computer application, the method comprising:

- creating a plurality of security policies, wherein each security policy specifies a level of security for the distributed computing system;
- distributing the plurality of security policies to each computer in the distributed computing system;
- selecting a specific security policy from the plurality of security policies for use across the distributed computing system; and
- informing each computer in the distributed computing system to use the specific security policy;

wherein the plurality of security policies includes a default security policy, wherein the default security policy is selected by a computer within the distributed computing system if the specific security policy is defective.

2. (Original) The method of claim 1, wherein the level of security includes a specific security posture.

3. (Original) The method of claim 1, further comprising using secure communications for distributing the plurality of security policies to each computer in the distributed computing system.

-3-

4. (Original) The method of claim 1, further comprising signing each security policy in the plurality of security policies with a cryptographic signature to allow detection of unauthorized changes.

5. (Original) The method of claim 1, further comprising distributing the plurality of security policies from a computer in the distributed computing system to a subordinate computer.

6. (Original) The method of claim 1, wherein selecting the specific security policy for use includes selecting the specific security policy based on a security posture.

7. (Original) The method of claim 6, wherein informing each computer in the distributed computing system to use the specific security policy includes using secure communications for distributing the security posture indicator to each computer in the distributed computing system.

8. (Cancelled)

9. (Currently Amended) A computer-readable storage medium storing instructions that when executed by a computer cause the computer to perform a method for managing security policies in a distributed computing system, wherein security policies determine access rights to a computer application, the method comprising:

creating a plurality of security policies, wherein each security policy specifies a level of security for the distributed computing system;
distributing the plurality of security policies to each computer in the distributed computing system;

selecting a specific security policy from the plurality of security policies for use across the distributed computing system; and

-4-

informing each computer in the distributed computing system to use the specific security policy;

wherein the plurality of security policies includes a default security policy, wherein the default security policy is selected by a computer within the distributed computing system if the specific security policy is defective.

10. (Original) The computer-readable storage medium of claim 9, wherein the level of security includes a specific security posture.

11. (Original) The computer-readable storage medium of claim 9, wherein the method further comprises using secure communications for distributing the plurality of security policies to each computer in the distributed computing system.

12. (Original) The computer-readable storage medium of claim 9, wherein the method further comprises signing each security policy in the plurality of security policies with a cryptographic signature to allow detection of unauthorized changes.

13. (Original) The computer-readable storage medium of claim 9, wherein the method further comprises distributing the plurality of security policies from a computer in the distributed computing system to a subordinate computer.

14. (Original) The computer-readable storage medium of claim 9, wherein selecting the specific security policy for use includes selecting the specific security policy based on a security posture.

-5-

15. (Original) The computer-readable storage medium of claim 14, wherein informing each computer in the distributed computing system to use the specific security policy includes using secure communications for distributing the security posture to each computer in the distributed computing system.

16. (Cancelled)

17. (Currently Amended) An apparatus that facilitates managing security policies in a distributed computing system, wherein security policies determine access rights to a computer application, the apparatus comprising:

a creating mechanism configured to create a plurality of security policies, wherein each security policy specifies a level of security for the distributed computing system;

a distributing mechanism configured to distribute the plurality of security policies to each computer in the distributed computing system;

a selecting mechanism configured to select a specific security policy from the plurality of security policies for use across the distributed computing system; and

an informing mechanism configured to inform each computer in the distributed computing system to use the specific security policy;

wherein the plurality of security policies includes a default security policy, wherein the default security policy is selected by a computer within the distributed computing system if the specific security policy is defective.

18. (Original) The apparatus of claim 17, wherein the level of security includes a specific security posture.

-6-

19. (Original) The apparatus of claim 17, further comprising a secure communications mechanism that is configured to distribute the plurality of security policies to each computer in the distributed computing system.

20. (Original) The apparatus of claim 17, further comprising a signing mechanism that is configured to sign each security policy in the plurality of security policies with a cryptographic signature to allow detection of unauthorized changes.

21. (Original) The apparatus of claim 17, wherein the distributing mechanism is further configured to distribute the plurality of security policies from a computer in the distributed computing system to a subordinate computer.

22. (Original) The apparatus of claim 17, wherein the selecting mechanism includes a policy selecting mechanism that is configured to select the specific security policy based on the security posture.

23. (Original) The apparatus of claim 22, wherein the informing mechanism includes a secure communications mechanism for distributing the security posture to each computer in the distributed computing system.

24. (Cancelled)

25. (New) The method of claim 1, wherein a host is provided including applications, a security posture interpreter, and a local policy database, the applications capable of registering with the security posture

-7-

interpreter, whereupon registration, the security posture interpreter returns a current security policy to the applications.

26. (New) The method of claim 25, wherein the security posture interpreter includes a posture access agent, a posture registration agent, and a posture notification agent, whereupon notification of a new security posture, the posture access agent determines a current security posture by accessing the current security policy within the local policy database, the posture access agent provides the current security posture to the posture notification agent, the posture registration agent provides access for the applications to register with the security posture interpreter, whereupon one of the applications registering with the posture registration agent, the application provides a call-back address so that the posture notification agent notifies the application when the current security posture changes.

27. (New) The method of claim 26, whereupon the posture notification agent receiving notification that the current security policy has changed, the posture notification agent notifies the registered applications of the change in the current security posture.

28. (New) The method of claim 27, wherein the local policy database includes a hierarchical data structure of directories and files, a top-level directory of the directories including a master policy with directories for a role authorization policy, an additional policy, and a security policy interpreter policy, the role authorization policy and additional policy including files which define the security policies for the role authorization policy and additional policy, each directory including multiple files, where each file specifies the security policy for a particular security posture.